UNITECH 2019 GABROVO

INTERNATIONAL SCIENTIFIC CONFERENCE
15 – 16 November 2019, GABROVO

ИЗСЛЕДВАНЕ НА СИГУРНОСТТА В БЕЗЖИЧНИ МРЕЖИ

STUDY OF WIRELESS NETWORKS SECURITY

Hristo Valchanov
Technical University of Varna

Veneta Aleksieva
Technical University of Varna

Jan Edikyan
Technical University of Varna

Abstract

Wireless network allow easy to build small enterprise and home networks based on IEEE 802.11 standard. The spreading of IoT is a prerequisite for a growing number of users worldwide. However, wireless networks are easily susceptible to attacks against their security. This requires an analysis of the problems and creating recommendations to improve their security. This paper presents a methodology and study of wireless network security in Varna city. The information was collected using the war-driving technique. The obtained results are analyzed and compared with those from previous studies.

Keywords: Wireless Security, Wi-Fi, War Driving.

ВЪВЕДЕНИЕ

Безжичните мрежи позволяват лесно изграждане на малки по размер както фирмени, така и домашни мрежи [1]. Отпадането на необходимостта от изграждане на кабелни трасета, допълнителни мрежови устройства, както и възможността за мобилност, са в основата на тяхното все по-масово използване в последните години. Навлизането на IoT е предпоставка за нарастването на броя на потребителите в световен мащаб. Типично, безжичните мрежи са базирани на стандарта IEEE 802.11 [2]. Технологиите са развиват непрекъснато, предоставяйки все по-големи скорости на потребителите. Но поради естеството на използване на радио сигнали, безжичните мрежи са лесно податливи на атаки срещу сигурността. Това може да включва както атаки от типа прекъсване на конекции, така и неоторизиран достъп до ресурси в дадена мрежа, откраднване на информация или скриване зад легитимна мрежа за провеждане на атаки срещу други мрежи. Една от основните задачи към мрежовата сигурност е изследване на рисковете и потенциалните уязвимости на Wi-Fi мрежите, което ще позволи дефиниране на препоръки към потребителите за подобряване на тяхната сигурност [3].

В настоящия доклад е представена методика и изследване на сигурността на безжични мрежи в района на град Варна. Информацията е събрана чрез използване на техниката war-driving. Получените резултати са анализирани и сравнени с тези от предишни изследвания.

ОСНОВНИ ПРИНЦИПИ

Безжичните мрежи се изграждат основно на базата на стандарта 802.11. Той включва множество стандарти, определящи използването на различни технологии за безжичен достъп, като се започне с 802.11a и скорост от 54Mbs до съвременния 802.11ah със скорост от 347Mbps [4]. Развитието на стандарта 802.11 е свързано и с развитие на протоколи за сигурност на безжични мрежи. Съществуват три основни протокола: WEP, WPA, WPA2 [5].

Wired Equivalent Privacy (WEP) – това е исторически първият протокол, позволяващ криптиране на връзката между безжични устройства на базата на предварително споделен ключ. Това е и основният му недостатък, позволяващ атакуващият след прехващане на голям брой пакети да получи този

ключ. Не се препоръчва неговото използване.

Wi-Fi Protected Access (WPA) – подобрява сигурността спрямо WEP. Предоставя два начина за контрол на достъпа: за персонално използване WPA Pre-Shared Key с дължина на ключа от 256Bit. За корпоративни решения се използва WAP Enterprise (802.1x) и автентикационен сървър. За осигуряване на интегритет на данните се използва TKIP, позволяващ динамично генериране на 128Bit ключове за всеки пакет. Въпреки подобренията се препоръчва използването на протокола WPA2.

WiFi Protected Access 2 (WPA2) е подобрена версия, по-устойчива на атаки. При нея се използва нов асиметричен алгоритъм за криптиране Advanced Encryption Standard (AES) и нов протокол заменящ TKIP – CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol).

Въпреки подобрената сигурност на WPA и WPA2 и двата имат един и същи проблем – възможна атака през Wireless Protected Setup (WPS) [6]. Това е стандарт, улесняващ конфигурирането на безжични устройства. Уязвимостта се изразява във възможността атакуващият в рамките на 2-4 часа да разбие използваната парола и да получи несанкциниран достъп до мрежата.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Целта на проведеното изследване е да се отговори на основния въпрос:

Какво е текущото състояние на сигурността при безжичните мрежи в района на град Варна?

Реализацията на целта изисква изпълнението на следните задачи:

- да се получи информация за голям брой безжични мрежи във Варна;
- да се определи процентното съотношение на криптираните мрежи;
- да се определят видовете производители и мрежите;
- да се определи процентното съотношение на използване на WPS.

За изпълнението на тези задачи изследването е проведено в няколко фази: разработване на система за анализ; събиране на информация; анализ на събраната информация; сравняване с предишни резултати.

ПРОЕКТИРАНЕ НА СИСТЕМАТА

Изследването на сигурността на безжични мрежи е процес извършван ръчно още от тяхното създаването, но поради множеството достъпна информация, той не е бил ефективен за използване в по-голям мащаб. Първите автоматизирани изследвания на сигурността на безжични мрежи са приложени в края на 1999г. в Калифорния, САЩ от Pete Shipley и представени за първи път на конференцията DEFCON-9 [7] през 2001г. Основния принцип представлява посещение на района, който ще бъде изследван и обхождането му (пеша, с велосипед или автомобил) с хардуер, способен да събира и записва информация излъчвана от безжичните точки за достъп, както и GPS информация за приблизителната тяхна позиция.

Настоящото изследване използва техниката war-driving с цел обхождане на по-големи райони за анализ [8, 9, 10]. Извършено е пасивно изследване, като изводи за сигурността се формулират единствено от публично достъпната информация, излъчвана от всяка точка на достъп в безжична мрежа [11].

Системата за събиране на данни е изградена на базата на едноплатков компютър Raspberry Pi 3 Model B, с процесор ARM Cortex-A53, 1.2GHz, вградена Wi-Fi и Bluetooth функционалност. За целта на реализацията е нужно записването на позицията на всяка безжична точка за достъп. Избраният GPS модул, поради поддръжка на стандарта NMEA 0183, дълготрайна батерия и голяма памет е Holux M-1200E.

За сканиране на безжичните мрежи се използва модул CanaKit Wi-Fi Module. За да се осигури продължително захранване на едноплатковия компютър, се използва портативна батерия Canyon CNS-TPBP5DG с капацитет 5000mAh (фиг.1).

***Фиг. 1**. Система за сканиране*

Сканирането на безжичните мрежи е реализирано посредством софтуер с отворен код Kismet. Софтуерът е компилиран и инсталиран под операционната система Raspbian OS. Получените от Kismet данни се записват в *netxml* формат. Събраната информация са конвертира чрез скрипт на Python в *csv* формат. Това е необходимо, за да могат данните да се представят в табличен вид с цел по-лесна обработка и анализ чрез Microsoft Excel.

СЪБИРАНЕ НА ДАННИ

Избраният район за анализ включва централната част на гр. Варна, тъй като в нея се намират по-голяма част от офисите и голяма част от живущите. Също така, районът съвпада с проведено подобно изследване от 2008г. [12], с цел сравнение на получените резултати (фиг.2).

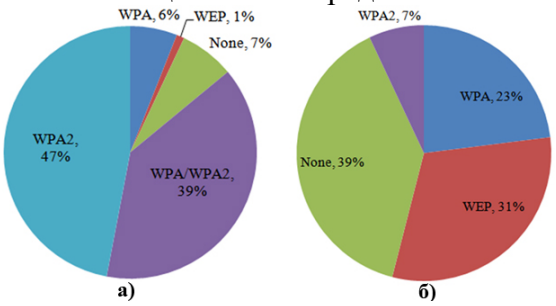
***Фиг. 2**. Сканиран район*

Обикалянето на района е извършено с автомобил с поддържана скорост в рамките на 0-35 км/ч. За да бъде наблюдаван и контролиран процеса в реално време, чрез Ethernet порта на Raspberry Pi се извършва връзка към лаптоп, на който благодарение на VNC клиент се наблюдава състоянието и информацията, представяна от Kismet (фиг. 3). Събраните данни включват информация за общо 19136 мрежи.

***Фиг. 3**. War-driving в действие*

WI-FI СИГУРНОСТ

Фигура 4-а представя процента на използваните методи за криптиране. Тези данни водят до обобщени резултати, показващи, че процентът на мрежите без или с WEP защита е пренебрежимо малък. Вероятна причина е използването на стари устройства или некомпетентност на потребителя за уязвимостта на WEP. Установено е, че 7% не използват криптиране. По-вероятно е това да са обществени мрежи с отворен достъп, отколкото те да не са конфигурирани. Това е характерно за ресторантите и магазините, както и за обществените градски зони.

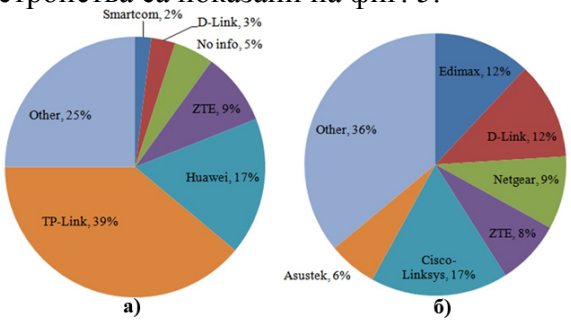


***Фиг. 4**. Използване на Wi-Fi криптиране през 2018 (а) и 2008 (б)*

Само 6% от мрежите, използват WPA, което е положително, но други 39% също го поддържат, тъй като освен протокола AES CCMP (показващ, че поддържат и WPA2), те поддържат и TKIP. По този начин, тези мрежи, които изглеждат сигурни (тъй като на пръв поглед са WPA2), всъщност се оказват несигурни, поради факта, че работят в смесен режим. В много случаи обаче смесеният режим е нужен, тъй като се поддържа от стари модели устройства, които не могат да работят с WPA2.

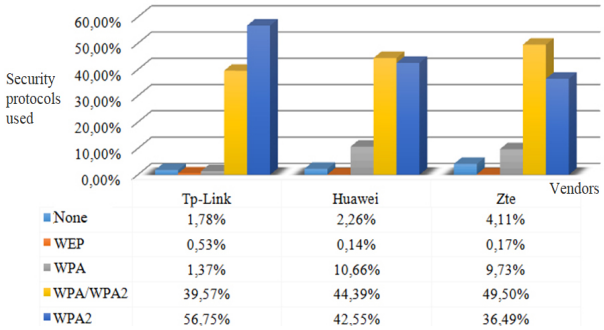
WI-FI ПРОИЗВОДИТЕЛИ

Най-често използваните марки Wi-Fi устройства са показани на фиг. 5.



***Фиг. 5**. Използвани марки устройства през 2018 (а) и 2008 (б)*

Видимо на първо място е марката TP-Link – причините за това, са както ниската цена, така и факта, че един от големите доставчици в града предоставя модели на това устройство безплатно на своите клиенти. При второ и трето място, Huawei и Zte, ситуацията е подобна – Mtel предоставя устройства Huawei, Vivacom преди е предоставял ZTE, а в последните години също Huawei. Въпреки това обаче, благодарение на по-добри настройки по подразбиране, единствено при TP-Link процентът на мрежи с метод на защита WPA2 е по-голям от комбинирания WPA/WPA2 (фиг.6).



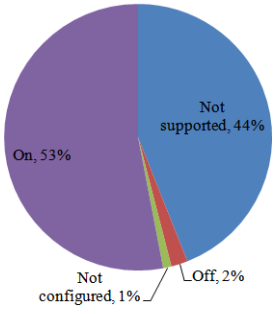
	Tp-Link	Huawei	Zte
None	1,78%	2,26%	4,11%
WEP	0,53%	0,14%	0,17%
WPA	1,37%	10,66%	9,73%
WPA/WPA2	39,57%	44,39%	49,50%
WPA2	56,75%	42,55%	36,49%

***Фиг. 6**. Сигурност при производители*

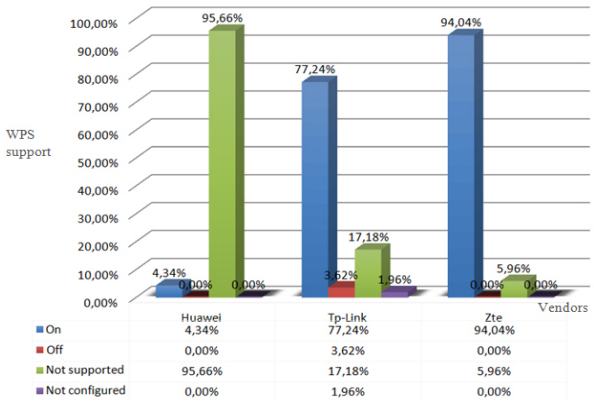
ИЗПОЛЗВАНЕ НА WPS

Следващите анализирани данни показват каква част от мрежите в гр. Варна предлагат функцията WPS. Тя е много важен фактор за сигурността, поради проблемите в технологията (фиг.7).

При анализ на поддръжката на WPS при топ марките, се забелязва факта, че при TP-Link 77% от устройствата дават възможност за използване на WPS. При Mtel и устройствата Huawei, по подразбиране WPS е изключен. При Vivacom и ZTE, ситуацията е обратната – WPS е по подразбиране включен (фиг. 8).



***Фиг. 7**. Използване на WPS*



	Huawei	Tp-Link	Zte
On	4,34%	77,24%	94,04%
Off	0,00%	3,62%	0,00%
Not supported	95,66%	17,18%	5,96%
Not configured	0,00%	1,96%	0,00%

***Фиг. 8**. Поддръжка на WPS при производители*

СРАВНЕНИЕ С РЕЗУЛТАТИ ОТ ПРЕДИШНО ИЗСЛЕДВАНЕ

Предишно проучване през 2008 [12] анализира данни за 688 мрежи. В сравнение с настоящия брой сканирани мрежи това означава, че за 10 години в града има значително увеличение на броя на мрежите – повече от 16 пъти. В допълнение, има и значително подобрение на мрежовата сигурност, както е показано на фиг.4-б.

Процентът на мрежите без каквато и да е защита е намалял почти 4 пъти, от 39% на 7%, а мрежите със защита на WEP са пренебрежимо малък брой (за разлика от над 30% през 2008г.). Използването на WPA е намаляло до само 6%. За разлика от това, увеличението е в полза на WPA2 (40% ръст) и WPA/WPA2 смесени устройства.

По отношение на доставчиците, ZTE е единствената запазена марка и дори е увеличила своя дял на пазара. Всички останали основни играчи през 2008г. вече имат пазарен дял под 5% (Cisco-Linksys има 2%, а D-Link – 3%). Получените по-рано резултати са представени на фиг.5-б.

Може да се обобщи, че за този период от 10 години нивото на сигурност е значително повишено. Сега 47% от мрежите в града използват стандарта WPA2, в сравнение със 7% от предишното проучване.

Изключително тревожен факт е обаче, че 59% от защитените WPA2 мрежи във Варна използват функцията WPS, което значително намалява тяхната сигурност. Известни са множество средства и програми, които позволяват на всеки лесно да извърши атака с няколко клика на мишката.

ЗАКЛЮЧЕНИЕ

Настоящият доклад представя проучване на сигурността на безжични мрежи, проведено в град Варна. Използвана е техника war-driving, базирана на разработена система за сканиране с Raspberry Pi. Получените резултати са сравнени с подобни, получени през 2008г.

Отговорът на поставения като основна цел на изследването въпрос може да се формулира така: *Резултатите показват значително увеличаване на сигурността на Wi-Fi мрежите в града, но въпреки това има какво още да се подобри в тази насока*.

Причините за подобряване на сигурността могат да се разгледат в две насоки. Първо, производителите предлагат устройства, които по подразбиране имат конфигуриран протокол WPA2. Второ, по-големите организации имат ИТ отдели, които се грижат за сигурността. Въз основа на резултатите за откритите SSID, смесен режим WPA/WPA2 и WPS, може да се заключи, че повечето от анализираните Wi-Fi мрежи принадлежат на обикновени потребители, които нямат достатъчно знания за сигурност.

Основните препоръки могат да бъдат представени в следните направления:

1. Да се използва само метод WPA2 за криптиране. В случай на по-стари устройства, за предпочитане е да се изгради отделна мрежа, която поддържа смесен режим WPA/WPA2.
2. Да се деактивира WPS за всички устройства.
3. Да се избира сложна парола.
4. Да се актуализира софтуера на устройствата до последната версия.
5. Да се информират потребителите за проблемите в сигурността на Wi-Fi мрежата.

Като насоки за бъдещата работа се предвижда анализ на най-новите мрежи 802.11ac и 802.11ah, както и проучване на нивото на сигурност в по-разширени райони на град Варна и региона.

ЛИТЕРАТУРА

[1] G. Colbach. Wireless Networking: Introduction to Bluetooth and WiFi. Independently published. 2017.

[2] IEEE 802.11 Wireles local area networks, http://www.ieee802.org/11/.

[3] S. Gopalakrishnan. A survey of wireless network security. IJCSMC, 1(3), 53–68. 2014.

[4] IEEE 802.11-2016 - IEEE Standard for Information technology. https://standards.ieee.org/standard/802_11-2016.html.

[5] NetSpot Wireless security protocols: WEP, WPA, WPA2, and WPA3, https://www.netspotapp.com/ wifi-encryption-and-security.html.

[6] S.Viehböck, Brute forcing Wi-Fi Protected Setup, https://sviehb.files.wordpress.com/ 2011/12 /viehboeck_wps.pdf.

[7] P.Shipley, 802.11b War Driving and Lan Jacking, https://www.defcon.org/html/defcon-9/defcon-9-speakers.html.

[8] D.Dobrilovic. A method for comparing and analyzing wireless security situations in two capital cities. Acta Polytechnica Hungarica, 3(13), 67–86. 2016.

[9] S.S.Sebbar (2016). An empirical study of WIFI security and performance in Morocco - wardriving in Rabat. DOI:10.1109/EITech.2016.7519621.

[10] K.A.Kyaw, Z.Tian and B.Cisak. Wi-Pi: a study of WLAN security in Auckland city. IJCSNS, 8(16), 68–80. 2016.

[11] S.U.Priya. The Impact of War Driving On Wireless Networks. IJCSET, 3(6), 230–235. 2013.

[12] H.Valchanov, I.Ruskov and A.Varbanov. A Study of the Wireless Network Security. Proc of “Computer Science 2009”, 273–278. 2009.